



MEETING THE PROJECT MANAGEMENT CHALLENGE

2004

Abstract

“Galileo/ASSAP: A Dynamic Fault Tree Analysis Tool”

Joanne Bechta Dugan

An important part of a Probabilistic Risk Assessment (PRA) methodology is the estimation of the probability of occurrence of an undesirable event; fault tree analysis (FTA) is often used to assess this probability. The use of FTA has been facilitated by improved mathematical analysis techniques as well as by sophisticated and easy to use software tools. Although FTA has wide applicability, it is an imperfect tool for reliability analysis of computer-based systems, because FTA cannot adequately model the complex failure behaviors associated with software-based systems.

Dynamic fault trees (DFT) extend traditional FTA to model complex failure behaviors, without compromising the ease-of-use associated with FTA. DFT adds a sequential notion to the traditional fault tree approach: system failures can depend on component failure order as well as combination. Special purpose dynamic fault tree gates can model dynamic replacement of failed components from pools of spares, failures that occur only if others occur in certain orders, dependencies that propagate failure in one component to others, and situations where failures can occur only in a predefined order.

This talk introduces the audience to DFT analysis, by way of several examples. We discuss the complexities inherent in software-based systems and the DFT models used to analyze reliability. DFT analysis is supported by Galileo, a software tool for dynamic fault tree analysis developed by the University of Virginia under contract to NASA. This talk will include a demo of Galileo.



NASA Project Management Conference